

**Healthuma Personal Unique Code (HPUC) Application Form
– Biometric Identity Verification**

Application Date:

(Month and Day)

(Year)

UFN 260206-0001

The following information is required to complete your HPUC application. Please truthfully provide all details requested below. Your information will be securely stored by Healthuma. To learn more about how we handle your personal data or to view our Privacy Statement, please visit our official website at www.healthuma.com.

PART I Legal Capacity Information

1. Name Identification	First Name	Last Name
2. Physiological Feature	Biological Gender	Date of Birth
	Country of Birth	

PART II Biological Credentials

3. Please upload your **Identification Photo**. Through the HPUC Application System
(a) Upload Format: JPG/PNG
(b) Size: 354×472px (2×2 inches)
(c) Requirement White background
. No obstruction
. Taken within the last 6 months

4. Electronic Signature	Please sign your name here		
5. Passport Certificate	Passport No.	Passport Issuing Country	Passport Expiry Date
	Please upload your Front Page Scan <u>Through the HPUC Application System</u> (a) Upload Format: PDF/JPG (b) Requirement <10MB		

NOTE 01 Suitable for The Crowd

Form 01-B serves as the core application document. Therefore, all individuals applying for the HPUC must complete this form, regardless of whether they are seeking the 72-hour HPUC or the formal HPUC.

NOTE 02 Description

Purpose

This form constitutes the foundation of the Health to Human International Medical Center's identity authentication system, aiming to establish a globally unique biometric digital identity profile for each patient. By integrating government-issued identification with multimodal biometric data, the system will generate a 12-digit Healthuma Personal Unique Code (HPUC) as your lifetime unique identifier for all medical activities at our center. This code will be encrypted and bound to your biometric templates such as facial features, ensuring absolute accuracy in identity verification and making it non-transferable.

Security

All submitted biometric data (including facial images and

electronic signatures) are transmitted via AES-256 encryption and stored in an isolated biometric database compliant with HIPAA and GDPR standards. Original images are securely destroyed after feature template extraction, and only non-reversible mathematical feature vectors are retained by the system. Data access is protected by a quadruple authentication mechanism, and any retrieval activity triggers real-time audit logging with simultaneous notification to the patient.

Exclusivity

The HPUC adheres to the "one person, one code" principle, is uniquely assigned for life, and is non-transferable. The Center strictly prohibits any form of identity sharing or proxy authentication. Accompanying persons must obtain temporary access credentials through an independent verification process,

with their permissions strictly limited to designated accompaniment areas and physically isolated from the patient's HPUC. Violation of identity exclusivity regulations will result in immediate termination of medical services and initiation of legal proceedings.

Integrity

You declare that the passport information, biometric data, and personal details submitted are true, accurate, and complete. Any false statement will result in immediate invalidation of the HPUC and may constitute medical fraud. The Center reserves the right to verify authenticity through Interpol databases and biometric cross-verification. Any identity discrepancies detected during the authentication process will trigger a 72-hour manual review.

Permanence

The HPUC remains permanently valid once generated and will not expire due to changes in address, nationality, or name. Biometric templates are automatically updated every 24 months to accommodate natural physiological changes, while the core identifier remains constant. Patients may request re-collection of biometric data through official channels at any time; however, the numeric sequence of the HPUC will never be altered, ensuring lifelong continuity of medical records.

Confidentiality

Your biometric profile is used solely for internal identity verification at our center and for rapid identification in emergency medical situations. Without your written authorization, raw biometric data will never be disclosed to any third party, including insurance companies, government agencies, or family members. In cases where disclosure is legally mandated, you will be notified in writing at least 72 hours in advance, and the scope of such disclosure will be strictly limited to the minimum necessary.

Sovereignty

You retain full sovereignty over your biometric data. You may, at any time, review records of its usage, download an encrypted copy of your profile, or request its complete deletion (except where legally required to be retained). Deletion requests will be processed within 30 days, including technical erasure, and a destruction certificate verified by a third-party audit authority will be provided. The Center does not claim any ownership of your biometrics.

Obligation

As a user of the exclusive high-net-worth medical service system, you are obligated to: securely maintain your personal authentication devices; promptly report any suspected identity misuse; and comply with the mandatory biometric update every five years. Failure to fulfill these obligations may result in temporary access restrictions until enhanced identity verification is completed.

Jurisdiction

This authentication agreement shall be governed by the laws of the State of New York, USA. The exclusive jurisdiction for any dispute resolution shall reside in the Federal District Court for the Upper East District of New York. The processing of biometric data shall also comply with the applicable laws of your country of nationality. In the event of any conflict of laws, the standard offering stricter protection shall prevail. All cross-border data

transfers are safeguarded through the European Union Standard Contractual Clauses (SCCs).

Commitment

Healthuma commits to strictly confining the use of biometric technology to enhancing medical safety and service efficiency. It will never be used for commercial marketing, behavioral analysis, or any non-medical purposes. We regard your biometrics as the most sensitive component of your health information and fulfill our data fiduciary duties with the same rigor as safeguarding life.